Method and device for generating antiforge authentication data, its authentication method and device, and its system

Publication number: CN1276659
Publication date: 2000-12-13
Inventor: YE JIQING (CN); JIANG TIAN (CN)
Applicant: YE JIQING (CN)
Classification:
- International: ***G06F17/00; G07F7/00; H04L9/00;*** **G06F17/00; G07F7/00; H04L9/00;** (IPC1-7): H04L9/00; G06F17/00; G07F7/00
- European:
Application number: CN19991007853 19990603
Priority number(s): CN19991007853 19990603

Also published as:
CN1175613C (C)

Abstract of **CN1276659**

A method for generating antiforge authenitication data of object includes generating ID data of object, providing the first monodirectional function and the first key, transforming the ID data to obtain authentication data, providing the second monodirectional function and the second key, combining data, transforming to obtain check data, and combining the authentication data with the check data.The device using said method and the authenticating method, device and system are also disclosed. Its advantages are quick authentication and high antiforge effect.

[19]中华人民共和国国家知识产权局

[51]Int.Cl⁷
H04L 9/00
G07F 7/00 G06F 17/00

[12]发明专利申请公开说明书

[21]申请号 99107853.5

[43]公开日 2000年12月13日

[11]公开号 CN 1276659A

[22]申请日 1999.6.3 [21]申请号 99107853.5
[71]申请人 叶季青
地址 100039 北京市丰台区郑常庄307号8室
共同申请人 江 天 陈 工
[72]发明人 叶季青 江 天

权利要求书6页 说明书12页 附图页数5页

[54]发明名称 生成防伪认证数据的方法与装置,其认证方法与装置及系统

[57]摘要

本发明提供一种生成物品防伪认证数据的方法,包括以下步骤:生成物品的标 识数据;提供第1单向函数和第1密钥;对该标识数据进行变换而生成认证数 据;提供第2单向函数和第2密钥;对合并数据进行变换而生成校验数据;以 及将这些数据合并为物品防伪认证数据。还提供应用该方法的装置、认证方法 与装置及其认证系统。将防伪数据和物品结合,在物品流通过程中,可用认证 装置对认证数据和校验数据进行实时、快速验证物品的真伪,且其防伪性强。

ISSN 1008-4274

权 利 要 求 书

1. 一种生成物品防伪认证数据的方法，包括：

标识数据生成步骤，根据物品特征和等级划分文件，生成一组唯一标识某一物品的标识数据；

提供第 1 单向函数和第 1 密钥的步骤；

认证数据生成步骤，根据提供的所述第 1 单向函数，在所述第 1 密钥的作用下，对所述标识数据进行变换，生成认证数据，且提供所述标识数据与所述认证数据的合并数据；

提供第 2 单向函数和第 2 密钥的步骤；

校验数据生成步骤，根据提供的所述第 2 单向函数，在所述第 2 密钥的作用下，对所述合并数据进行变换，生成校验数据；以及

防伪数据合成步骤，将所述标识数据、所述认证数据和所述校验数据，合并为物品防伪数据。

2. 根据权利要求 1 所述的生成防伪认证数据的方法，其特征是所述提供第 1 单向函数和第 1 密钥的步骤包括所述单向函数对整个信息或密钥的任一比特数进行改变时，所得认证数码有规定的比特发生变化。

3. 根据权利要求 2 所述的生成防伪认证数据的方法，其特征是所述提供第 1 单向函数和第 1 密钥的步骤还包括：

对所提供的所述单向函数进行检测的步骤，使得对给定信息 x 和相应的变换 f(x)，寻求伪信息 x′ 使 f(x′)=f(x)的难度足够大；以及

对于任意的 x, x1 和 x2，$f(x1 \cdot x2) \neq f(x1) \cdot f(x2)$，$f(x) \neq cx$，$f(x) \neq x^a$，其中 c 为任意常数，a 为任意常数。

4. 根据权利要求 2 或 3 所述的生成防伪认证数据的方法，其特征是所述提供第 1 单向函数和第 1 密钥的步骤，还包括：选定 32

比特≤X,M,p≤160 比特，将 X,p 作为密钥 k 秘密保存于存储器中并以 M 为唯一标识某物品的数据的选择步骤；算出 $Y=M^X+\beta \pmod p$ 值的计算步骤；以及对 $M^X+\beta \pmod p$ 的值采用截取的运算，使之处于 32 比特≤Y≤128 比特之间的截取步骤。

5. 根据权利要求 2 或 3 所述的生成防伪认证数据的方法，其特征是所述提供第 1 单向函数和第 1 密钥的步骤，还包括：选定 k1,k2,k3 作为密钥，设定 M 为要加密信息的一个固定长度的一段分组，使之满足 32 比特≤M,k1,k2,k3≤128 比特的选择步骤；算出 Y=DES（DES（DES(M,k1),k2）,k3）的计算步骤（假设单向函数为分组为 128 比特的类 DES）；以及对 Y 采用截取运算，使之处于 32 比特≤Y≤128 比特之间的截取步骤。

6. 根据权利要求 2 或 3 所述的生成防伪认证数据的方法，其特征是所述提供第 2 单向函数和第 2 密钥的步骤，还包括：选定 32 比特≤x,M_i,p,b≤64 比特，以 x,p 作为密钥 k 秘密保存于存储器中，以 b 为权值，M 为唯一标识某物品的数据和认证数据的合并值，当 M 大于 b 时，将 M 拆为多个 M_i，使各 M_i 均小于 b，即 $M=M_{e-1}*b^{e-1}+M_{e-2}*b^{e-2}+\cdots+M_{e-i}*b^{e-i}+\cdots+M_1*b+M_0$，其中 e 为 M 的长度对 b 的长度的倍数向上取整值的选择步骤；计算

$Z'=((\cdots((x^{M_e}+\beta)\bmod p)^{M_{e-1}}\bmod p\cdots)^{M_{e-i}}+\beta)\bmod p$ 的计算步骤；以及对 Y'的值采用截取运算，使之处于 12 比特≤Z≤32 比特之间的截取步骤。

7. 一种生成物品防伪认证数据的装置，其特征是备有：

标识数据生成部分，用于根据具有物品特征和等级划分文件，生成一组唯一标识某一物品的标识数据；

第 1 存储器，用于存储第 1 单向函数和第 1 密钥；

认证数据生成部分，用于按照所述第 1 单向函数，在所述第 1

密钥的作用下，对所述标识数据进行变换，生成认证数据，和输出上述标识数据与上述认证数据的合并数据；

第 2 存储器，用于存储第 2 单向函数和第 2 密钥；

校验数据生成部分，用于按照所述第 2 单向函数，在所述第 2 密钥的作用下，对所述合并数据进行变换，生成校验数据；以及

防伪数据合成部分，用于将所述标识数据、所述认证数据和所述校验数据，合并为物品防伪数据。

8. 根据权利要求 7 所述的生成防伪认证数据的装置，其特征是所述第 1 单向函数是，一种在函数 f 域中的任一自变量 X，计算相应的 f（X）值是容易的，但对 f 值域内几乎所有的 Y 和相应的 X，f（X）= Y，寻求一个适当的自变量 X′ 使 f（X′）= f（X）在计算上几乎是不可行的函数。

9. 根据权利要求 8 所述的生成防伪认证数据的装置，其特征是所述单向函数为 $Y=M^X+\beta \pmod p$，β 为大于零且小于 p 的常数。

10. 根据权利要求 9 所述的生成防伪认证数据的装置，其特征是所述第 1 单向函数的输入长度为 X 比特，输出为 Y 比特，X 和 Y 分别满足条件：32 比特≤X≤160 比特 ，32 比特≤Y≤128 比特。

11. 根据权利要求 8 所述的生成防伪认证数据的装置，其特征是所述单向函数为 Y=DES（DES（DES(M,k1),k2),k3），其中 k1,k2,k3 为密钥，M 是要被变换信息的一个固定长度的一段分组，32 比特≤M,k1,k2,k3≤128 比特。

12. 根据权利要求 8 所述的生成防伪认证数据的装置，其特征是所述第 2 单向函数为：

$Z = (\cdots((x^{M_0}+\beta) \bmod p)^{M_1} \bmod p \cdots)^{M_{n-1}}+\beta) \bmod p$

其中以 x,p 作为密钥 k，以 b 为权值，M 为唯一标识某物品的数据和认证数据的合并值；当 M 大于 b 时，将 M 拆为多个 M_i，使各 M_i

均小于 b，即 $M=M_{e-1}*b^{e-1}+M_{e-2}*b^{e-2}+\cdots+M_{e-j}*b^{e-j}+\cdots+M_1*b+M_0$，其中 e 为 M 的长度对 b 的长度的倍数向上取整值。

13. 根据权利要求 12 所述的生成防伪认证数据的装置，其特征是所述第 2 单向函数 Z 比特满足条件 12 比特≤Z≤32 比特。

14. 一种对物品上防伪认证数据进行认证的方法，包括下列步骤：

采集防伪数据，包括在物品上或物品包装上的唯一标识某物品的标识数据、认证数据和校验数据；

用规定的第 2 单向函数，对所述的标识数据和认证数据进行变换，得到变换的结果；

将所得结果和标识的所述校验数据进行比较，如不同则确认为该物品为假冒物品。

15. 根据权利要求 14 所述的认证方法，还包括步骤：

远程传输所述信息；

用规定的第 1 单向函数，对所述的标识数据进行变换（计算），得到变换的结果；

将所得结果和标识的所述认证数据进行比较，如不同则确认为该物品为假冒物品；

如相同则将该物品唯一标识的数据记录到装置的内存中，当该物品唯一标识的数据是第一次记录到内存时，认为该物品为真品，否则为伪品；以及

输出物品真伪的验证结果。

16. 一种对物品上防伪认证数据进行认证的装置，其特征是备有：

物品防伪数据输入部分，用于采集防伪数据，包括标识数据、认证数据和校验数据；

第 2 存储器，用于提供规定的第 2 单向函数和第 2 密钥；

第 2 数据变换器，用规定的第 2 单向函数，对所述的标识数据和认证数据进行变换（计算），得到变换后的数据；

第 2 比较器，用于将所述结果和输入的所述校验数据进行比较，如不同则确认为该物品为假冒物品。

17. 根据权利要求 16 所述的认证装置，其特征是备有：

物品防伪数据传输系统，用于传输所述采集的物品防伪数据；

第 1 存储器，用于提供规定的第 1 单向函数和第 1 密钥；

第 1 数据变换器，用所述第 1 单向函数和所述第 1 密钥，对所述的标识数据和认证数据进行变换（计算），得到变换后的数据；

第 1 比较器，用于将所述结果和输入的所述认证数据进行比较，如不同则确认为该物品为假冒物品；

数据记录到装置，当所述比较结果相同时，则将该物品唯一标识的的内存中，当该物品唯一标识的数据是第一次记录到内存时，认为该物品为真品，否则为伪品；以及

传输显示装置，用于传输和显示物品真伪的认证结果。

18. 一种物品防伪认证系统，其特征是具备：

物品防伪数据生成和分发中心，设有生成物品防伪数据的装置，用以生成物品防伪数据，并分发防伪数据；

物品生产厂家，将所述的防伪数据与物品相结合；

流通环节，具有防伪数据的物品进入用户；

物品防伪数据输入装置，用于在流通过程中采集物品防伪数据；

物品防伪数据传输系统，用于汇集防伪数据进行认证处理；以及

物品防伪数据认证中心，进行认证，并提供认证结果。

19. 根据权利要求 18 所述物品防伪认证系统，其特征是所述防

伪数据输入装置是电话装置或计算机网络具有信息回放或查询功能。

20. 根据权利要求 18 所述物品防伪认证系统，其特征是，所述物品防伪数据生成及认证中心，接受物品防伪密钥生成管理中心控制。

21. 根据权利要求 18 所述物品防伪认证系统，其特征是所述物品防伪数据的表现形式为十进制数据、十六进制数据，计算机通用字符，一维条码，二维条码中的一种形式。

22. 根据权利要求 18 所述物品防伪认证系统，其特征是所述的物品防伪数据和物品的结合方式是制作防伪数据标签，粘贴在物品或物品的（商标）标签上；打印在物品的（商标）标签上；印制在物品自身上；印制在物品的包装上或包装内；印制在物品容器上的一种方式。

23. 根据权利要求 18 所述物品防伪认证系统，其特征是所述物品防伪数据分发方式包括：（1）实物分发，将物品防伪数据印制在标签物体上进行分发；（2）信息传输分发，将物品防伪数据表示为二进制信息流，加密后，通过通信网络，传送物品防伪数据；（3）介质分发，将物品防伪数据表示为信息文件，写入记录介质中来分发物品防伪数据。

说　　明　　书

生成防伪认证数据的方法与装置,其认证方法与装置及系统

本发明涉及一种生成物品防伪认证数据的方法与装置，其认证的方法与装置及防伪认证系统，特别是，涉及利用单向函数原理生成一种特定的物品防伪认证数据的方法与使用该方法的装置，其认证的方法与装置及认证系统。

防伪认证方法是，用特定的装置生成防伪数码，并将防伪数码和物品结合起来，在物品流通的源头将一组物品防伪数码标识在物品上，在物品流通中或流通的终结处，用相应的装置对认证数码和校验数据码进行验算，达到鉴别物品的真伪。由于验证物品真实性的过程是一个单方向的过程，可用密码学上的单向函数来实现。

利用数据编码的方法生成物品防伪数码，用于商品的防伪或认证个人身份等已是众所周知的技术，例如 CN96118567.8 号，名称为“认证号码分发装置及认证号码验证装置”的专利和 CN97107763.0 专利，名称为“数码防伪法”的专利。这两个专利所揭示的生成认证数码和防伪数码的装置中，都利用了密码编码原理，并用之于商品防伪或身份认证。在实际应用中，要认证和防伪可靠，这些装置所基于的密码变换算法必须不可破译，而且是分组密码算法。

并且，上述的 96118567.8 号专利中，代码变换装置输入为 n 字符，输出也为 n 字符，而在 97107763.0 专利中，防伪数码生成装置或软件，输出和输入的长度也相等，即两者都要求输入和输出是一一对应的。从密码变换函数设计的角度看，若要敌手不能由可见的标识数据、认证数据计算出单向函数所用的密钥，所基于的密码算法必须是实际上不可破译的。密码变换算法的分组要求较长，一般至少 64 比特以上，若换算成十进制数，则达 20 位以上。如再加上其它，如校验数据、标识所用密钥的数据等，实际防伪数据

较长而且是长度固定的。如果采用强度较高的分组密码算法，其分组长度一般至少为 128 比特，防伪数据至少要 40 比特以上。而实际应用中，对网络传输的信道带宽、防伪数据录入方便程度等提出了很高的要求。

本发明就是为克服现有技术中的缺点而研发的，其目的在于提供一种依据物品的贵重等级，给出其唯一标识数据长度和防伪数据长度均不同，而防伪强度高、商业运营成本低和录入方便的生成物品防伪认证数据的方法与装置，其认证的方法与装置，及其防伪认证系统。

为了达到上述目的，根据本发明的生成物品防伪认证数据的方法，包括下列步骤：标识数据生成步骤，根据物品特征和等级划分文件，生成一组唯一标识某一物品的标识数据；提供第 1 单向函数和第 1 密钥的步骤；认证数据生成步骤，根据提供的所述第 1 单向函数，在所述第 1 密钥的作用下，对所述标识数据进行变换，生成认证数据，且提供所述标识数据与所述认证数据的合并数据；提供第 2 单向函数和第 2 密钥的步骤；校验数据生成步骤，根据提供的所述第 2 单向函数，在所述第 2 密钥的作用下，对所述合并数据进行变换，生成校验数据；以及防伪数据合成步骤，将所述标识数据、所述认证数据和所述校验数据，合并为物品防伪认证数据即防伪数据。

并且，根据本发明的生成物品防伪数据的装置，其中备有：标识数据生成部分，用于根据具有物品特征和等级划分文件，生成一组唯一标识某一物品的标识数据；第 1 存储器，用于存储第 1 单向函数和第 1 密钥；认证数据生成部分，用于按照所述第 1 单向函数，在所述第 1 密钥的作用下，对所述标识数据进行变换，生成认证数据，和输出上述标识数据与上述认证数据的合并数据；第 2 存储器，用于存储第 2 单向函数和第 2 密钥；校验数据生成部分，用于按照所述第 2 单向函数，在所述第 2 密钥的作用下，对所述合并数据和进行变换，生成校验数据；以及防伪数据合成部分，用于将所述标识数据、所述认证数据和所述校验数据，合并为物品防伪数据。

并且，根据本发明的对物品上防伪数据进行认证的方法，包括下列步

骤:采集防伪数据，包括在物品上或物品包装上的唯一标识某物品的标识数据和认证数据；用规定的第 1 单向函数，对所述的标识数据进行变换，得到变换的结果；将所得结果和标识的所述认证数据进行比较，如不同则确认为该物品为假冒物品；如相同则将该物品唯一标识的数据记录到装置的内存中，当该物品唯一标识的数据是第一次记录到内存时，认为该物品为真品，否则为伪品；以及显示物品真伪的验证结果。

并且，根据本发明的对物品上防伪数据进行认证的装置，其中包括：物品防伪数据输入部分，用于采集防伪数据，包括标识数据、认证数据和校验数据；第 2 存储器，用于提供规定的第 2 单向函数和第 2 密钥；第 2 数据变换器，用规定的第 2 单向函数，对所述的标识数据和认证数据进行变换（计算），得到变换后的数据；第 2 比较器，用于将所述结果和输入的所述校验数据进行比较，如不同则确认为该物品为假冒物品。

并且，上述认证的装置包括：物品防伪数据传输系统，用于传输所述采集的物品防伪数据；第 1 存储器，用于提供规定的第 1 单向函数和第 1 密钥；第 1 数据变换器，用所述第 1 单向函数和所述第 1 密钥，对所述的标识数据和认证数据进行变换，得到变换后的数据；第 1 比较器，用于将所述结果和输入的所述校验数据进行比较，如不同则确认为该物品为假冒物品；数据记录到装置，当所述比较结果相同时，则将该物品唯一标识的的内存中，当该物品唯一标识的数据是第一次记录到内存时，认为该物品为真品，否则为伪品；以及传输显示装置，用于传输和显示物品真伪的认证结果。

并且，根据本发明的物品防伪认证系统，其中包括：物品防伪数据生成和分发中心，设有生成物品防伪数据的装置用以生成物品防伪数据，并由该中心分发防伪数据；物品生产厂家，将所述的防伪数据与物品相结合；流通环节，使具有防伪数据的物品进入用户；物品防伪数据输入装置，用于在流通过程中采集物品防伪数据；物品防伪数据传输系统，用于汇集防伪数据进行认证处理；以及物品防伪数据认证中心，进行认证，并提供认证结果。

根据本发明的上述方案，与现有的防伪技术的主要不同之处，在于生成物品防伪数据（或称之为认证号码、防伪数码等）的方法与装置以及防伪数据组成结构不同。

本发明的物品防伪数据是唯一标识物品的数据、认证数据和校验数据的拼接。本发明对不同物品给出不同的标识数据，考虑到防伪装置内部运算起点（密钥）的不可逆推性，即密码变换函数的强度和防伪数据的长短实用性，依据物品唯一标识数据中标识的物品等级划分（依据物品的贵重程度），采用第 1 单向函数，将物品唯一标识数据压缩为长度不等的认证数据；然后再对物品唯一标识数据和认证数据用第 2 单向函数进行变换，生成长度更短的固定长度的物品的校验数据。

并且，本发明综合考虑到防伪强度、商业运营成本和方便录入等情况，比如，对商品而言，常见的商品防伪数据长度可较短，如为 24 位十进制数，相当于 3 个 8 位电话号码长，使用户可以忍受拨号的长度和时间。对于较贵重的商品或新技术产品，其防伪数据长度可较长，如为 30 位十进制数或更长。另外，验证装置可以是通过信息回放提示形式，提示用户输入商品防伪数据，电话装置可赋有信息回放功能，用户可以验证其输入的物品防伪数据的正确性并得到商品真伪的验证结果。

总之，本发明的生成物品防伪数据的方法与装置，其认证方法和装置及其系统具有防伪强度高、商业运营成本低、录入方便和认证快速可靠的优点。

下面，结合各附图，详细说明本发明的最佳实施例，使本发明的上述目的、特征和优点变得更清楚。

图 1 是表示本发明的生成防伪数据的方法的流程图。

图 2 是本发明的生成防伪数据装置的结构示意图。

图 3 是表是示物品认证方法的工作流程图。

图 4 是物品防伪系统组成示意图。

图 5 是集中式认证网络示意图。

在本发明中生成防伪数据包括：一组唯一标识某物品的数据，该数据可包括防伪数据的生产日期、有效期、厂家、产品名称等物品的特征信息，还可根据物品的普遍性和贵重性进行等级划分，对于不同种类的物品其唯一标识物品的数据长度通常相等；对唯一标识某物品的数据用单向函数 1 进行变换，变换的结果为认证数据，对于不同种类的物品其认证数据的长度不相等；以及将唯一标识某物品的数据和认证数据合并之后，用单向函数 2 进行变换，变换的结果为校验数据。并且，把唯一标识某物品的数据、认证数据和校验数据合起来称作物品防伪认证数据或防伪数据。

本发明的生成防伪数据的方法，如图 1 所示。

由于验证物品真伪性的过程通常是一个单向操作的过程，防伪数据生成装置采用单向函数原理，生成防伪数据的步骤包括：

第 1 步骤 S1，在标识数据生成部分中，生成一组唯一标识某物品的数据，即明码 P。对于不同物品，可具有不同长度的标识数据 P，该数据的长度在 32 至 160 比特之间，即 $32 \leqslant P \leqslant 160$ 比特。

该标识数据生成部分所生成的标识数据 P 送到认证数据生成部分和防伪数据合成部分中。

在第 2 步骤 S2，认证数据生成部分，接收来自标识数据生成部分输出的唯一标识某物品的数据 P，用来自第 1 存储器的第 1 单向函数，在第 1 密钥 K1 的作用下，对标识数据 P 进行变换，变换的结果生成认证数据 Y。不同物品的认证数据 Y 的长度不同，其长度在 32 至 128 比特之间，即 $32 \leqslant Y \leqslant 128$ 比特。

该认证数据生成部分把所生成的认证数据 Y 与上述标识数据 P 一起，送到校验数据生成部分中，同时把认证数据 Y 送到防伪数据合成部分中。

在第 3 步骤 S3，在校验数据生成部分中，将唯一标识某物品的数据 P

和认证数据 Y 合并之后，用来自第 2 存储器的第 2 单向函数，在第 2 密钥 K2 的作用下，对标识数据 P 和 Y 进行变换，变换的结果生成校验数据 Z。对不同物品也可以具有不同长度的校验数据 Z，其长度在 12 至 32 比特之间，即 12≤Z≤32 比特。

该校验数据生成部分把所生成的校验数据 Z，送到防伪数据合成部分中。

在第四步骤 S4，在防伪数据合成部分中，将分别来自标识数据生成部分、认证数据生成部分和校验数据生成部分的唯一标识某物品的数据 P、认证数据 Y 和校验数据 Z 合成为物品防伪数据。

根据本发明的生成物品防伪数据的方法而构成的本发明的生成物品防伪数据的装置，其中包括：标识数据生成部分，用于根据具有物品特征和等级划分文件，生成一组唯一标识某一物品的标识数据；第 1 存储器，用于存储第 1 单向函数和第 1 密钥；认证数据生成部分，用于按照所述第 1 单向函数，在所述第 1 密钥的作用下，对所述标识数据进行变换，生成认证数据，和输出上述标识数据与上述认证数据的合并数据；第 2 存储器，用于存储第 2 单向函数和第 2 密钥；校验数据生成部分，用于按照所述第 2 单向函数，在所述第 2 密钥的作用下，对所述合并数据和进行变换，生成校验数据；以及防伪数据合成部分，用于将所述标识数据、所述认证数据和所述校验数据，合并为物品防伪数据。

由本发明的上述生成防伪数据的方法和装置所生成的认证数据的长度 Y 加上校验数据的长度 Z，一般小于唯一标识物品的数据长度 P，即输入长度大于输出长度，变换不是一一对应的，也就是说，不同的输入可以对应相同的输出。本发明的方法和装置将输入的信息进行了压缩，由输出逆推出输入是不可能的。因此，本发明的安全系数高，可信任度大。

本发明对单向函数的主要要求包括：

1. 单向函数应对整个信息比特进行计算，信息或密钥的任一比特数改变时，所得认证码希望有一半的比特表示发生变化（信息用二进制形式时的变

化量）；

2. 对于给定信息 x 和相应的变换 f(x)，寻求伪信息 x′ 使 f(x′)=f(x)的难度足够大；

3. 对于任意的 x, x1 和 x2，f(x1 • x2)≠f(x1) • f(x2)，f(x)≠cx，f(x)≠x^a，其中 c 为任意常数，a 为任意常数；

4. 易于实现高速计算，便于用硬件或软件实现。单向函数可对任意长的信息进行变换，得到一个较短的固定长度的数据，要从该数据得到原来的信息是很难的或根本不可能的，因为这一变换函数可能是不可逆的，所以它具有单向特点。由于这一变换将较长的唯一标识某物品的数据信息变换为较短的认证数据和校验数据，数据量大大减少，也称该单向函数为压缩函数。

上面，已经说过，本发明的物品防伪数据由唯一标识各物品的数据、认证数据、校验数据三部分组成。认证数据是用第 1 单向函数对唯一标识各物品的数据进行变换运算的结果，而校验数据是用第 2 单向函数 2 对唯一标识各物品的数据和认证数据进行变换运算的结果，所以采用什么样的单向函数，对认证和防伪可靠性和所基于的密码变换算法影响很大。

下面，根据上述的要求，举例具体说单向函数。

本发明的第 1 单向函数，例如可以设定为，函数的输入长度为 X 比特，输出为 Y 比特，且 X 和 Y 分别满足条件：32 比特≤X≤160 比特 ，32 比特≤Y≤128 比特。这里的单向函数是指：对 f 域中的任一自变量 X 来说，计算相应的 f（X）值是容易的，但对 f 值域内几乎所有的 Y 和相应的 X，f（X）= Y 来说，寻求一个适当的自变量 X′，使 f（X′）= f（X），在计算上几乎是不可行的。

众所周知，大整数离散对数计算是数学难题，利用大整数模指数运算，可以构成一个单向函数，如 $Y=M^X+\beta \pmod p$，β 为大于 0 且小于 p 的常数。只要 Y, X, M, p 取足够大，已知 Y, M, p，很难求 X。

本发明的第 1 单向函数可用三个步骤构成：首先，选定 32 比特≤X, M, p

≤160 比特；将 X,p 作为密钥 k，秘密进行保存；并以 M 为唯一标识某物品的数据。其次，计算 $M^X+\beta \pmod p$ 的值；接着，对 $M^X+\beta \pmod p$ 的值采用截取的运算，使之处于 32 比特≤Y≤128 比特之间。

本发明的第 1 单向函数除了用上述的方法构成外，还可以用高强度的分组密码算法构成，例如用三重 DES 算法。该方法为：首先选定 k1,k2,k3 作为密钥，设 M 为要加密信息的一个固定长度的一段分组，满足 32 比特≤M,k1,k2,k3≤128 比特；其次计算 Y=DES（DES（DES(M,k1),k2）,k3）；而后对 Y 采用截取运算，使之处于 32 比特≤Y≤128 比特之间。

由上述方法得到的第 1 单向函数和第 1 密钥，被存储于第 1 存储器中，待用。

其次，举例说明本发明的第 2 单向函数。第 2 单向函数用三个步骤构成：首先，选定 32 比特≤x,M_i,p,b≤64 比特，以 x,p 作为密钥 k 并予以秘密保存，以 b 为权值，M 为唯一标识某物品的数据和认证数据的合并值；当 M 大于 b 时，将 M 拆为多个 M_i，使各 M_i 均小于 b，即 $M=M_{e-1}*b^{e-1}+M_{e-2}*b^{e-2}+\cdots+M_{e-i}*b^{e-i}+\cdots+M_1*b+M_0$，其中 e 为 M 的长度对 b 的长度的倍数向上取整值；其次，计算：

$Z'=((\cdots((x^{M_0}+\beta)\bmod p)^{M_1}\bmod p\cdots)^{M_{e-1}}+\beta)\bmod p$；

然后，对 Y′ 的值采用截取运算，使之处于 12 比特≤Z≤32 比特之间。

同样，由上述方法得到的第 2 单向函数和第 2 密钥，被存储于第 2 存储器中，待用。

本发明的物品防伪认证的工作流程，如图 3 所示。对认证数据进行验证的方法，包括下列步骤：

采集标识在物品上或物品包装上的唯一标识某物品的数据，在步骤 S11，用与上述同样的第 2 单向函数，对其中的标识数据和认证数据进行变换（计算），得到变换的结果 Z′。

在步骤 S12，将所得结果 Z′ 和标识在物品上或物品包装上的认证数据

进行比较，如 No 即不同，则转向步骤 S13，确认为该物为假冒物品或输入出错；如 Yes 即相同，则进入步骤 14，将该物品唯一标识的数据，通过远程传输的例如网络、电话之类传输到物品防伪数据认证过程中心，进行步骤 S15。

在步骤 S15，用与上述同样的第 1 单向函数，对标识数据进行变换（计算），得到结果为 Y′，然后进入步骤 S16。

在步骤 S16，将所得结果 Y′ 和标识在物品上或物品包装上的认证数据进行比较，如 No 即不同，则转向步骤 S19，确认为该物为假冒物品；如 Yes 即相同，则进入步骤 17。

在步骤 S17，判断该物品唯一标识的数据是否是“首次认证”，伪品，如 No 即不同，则转向步骤 S19，确定为该物为假冒物品；如 Yes 即相同，则进入步骤 18，认证为真品。也就是，将该物品唯一标识的数据记录到装置的内存中，当该物品唯一标识的数据是第一次记录到内存时，认为该物品为真品，其它为伪品。并且，向用户输出商品真伪的验证结果。

并且，应用本发明的对物品上防伪数据进行认证的方法而构成的一种对物品上防伪数据进行认证的装置，其中包括：物品防伪数据输入部分，用于采集防伪数据，包括标识数据、认证数据和校验数据；第 2 存储器，用于提供规定的第 2 单向函数和第 2 密钥；第 2 数据变换器，用规定的第 2 单向函数，对所述的标识数据和认证数据进行变换（计算），得到变换后的数据；第 2 比较器，用于将所述结果和输入的所述校验数据进行比较，如不同则确认为该物品为假冒物品。

根据本发明的认证装置，还包括:物品防伪数据传输系统，用于传输所述采集的物品防伪数据；第 1 存储器，用于提供规定的第 1 单向函数和第 1 密钥，第 1 数据变换器，用所述第 1 单向函数和所述第 1 密钥，对所述的标识数据和认证数据进行变换（计算），得到变换后的数据；第 1 比较器，用于将所述结果和输入的所述校验数据进行比较，如不同则确认为该物品为假

冒物品；数据记录到装置，当所述比较结果相同时，则将该物品唯一标识的的内存中，当该物品唯一标识的数据是第一次记录到内存时，认为该物品为真品，否则为伪品；以及传输显示装置，用于传输和显示物品真伪的认证结果。

图 4 示出了按照本发明的方法构成的物品防伪系统组成的示意图。如图 4 所示，在物品防伪数据生成和分发中心 1，按照上面说过的方法，生成物品的防伪数据并将这些物品防伪数据，分发给物品生产厂家 2。

物品防伪数据分发给物品生产厂家后，由物品生产厂家 2，将所述的物品防伪数据以多种表现形式，如十进制数据、十六进制数据、计算机通用字符、一维条码以及二维条码等与物品结合起来。这种结合有多种方式，例如，可以是制作防伪数据标签，粘贴在物品或物品的（商标）标签上；打印在物品的（商标）标签上；印制在物品自身上；印制在物品的包装上或包装内；印制在物品容器上等等。

物品防伪数据的分发也可以有多种方式，通过例如，实物分发，将物品防伪数据印制在标签物体上，通过分发具有物品防伪数据的标签，来分发物品防伪数据；信息传输分发，将物品防伪数据表示为计算机二进制信息流，通过现代计算机通信网络，传送物品防伪数据；介质分发，将物品防伪数据表示为计算机信息文件、二进制信息块，写在计算机磁盘、磁带上，EPROM、EEPROM、FLASH 芯片等介质中，通过传送磁盘、磁带、芯片来分发物品防伪数据。

物品的防伪数据在和物品结合前需保密分发和保管。在实物分发时，用管理方式进行对具有物品防伪数据的标签进行保密传送。物品防伪数据用信息传输分发和介质分发方式分发时，采用加密技术对所分发的防伪数据信息进行加密，并用公开密钥密码进行数据完整性检验、防伪数据分发处的信源鉴别和防伪数据接收处的信宿鉴别。

带有防伪数据标签之类的物品，从物品生产厂家 2 进入货物流通环节 3。

在流通过程中，商家或用户对物品的真伪如有怀疑，可借助于物品防伪数据输入装置 4，输入物品防伪数据。该物品防伪数据，以信息流的方式，通过物品防伪数据传输系统 5，例如，利用现代通信网络和数据库，将物品防伪数据快速汇集到物品防伪数据认证中心 6 进行验算认证，并立即将认证结果反馈到需要对防伪认证数据进行认证的地点，提供给用户。而且，防伪数据输入装置 4（即验证装置）可以是通过信息提示形式，提示用户输入商品防伪数据，若为电话装置可赋有信息回放功能，用户可以验证其输入的物品防伪数据的正确性并得到商品真伪的验证结果。

另外，上述的物品防伪数据生成与分发中心 1 和物品防伪数据认证过程中心 6 的工作，接受物品防伪密钥生成管理中心 7 控制。

如上所说，通常将防伪数据和物品结合起来，即在物品流通的源头将一组物品防伪数据标识在物品上。在物品流通中或流通的终结处，用相对应的装置，对一组物品防伪数据标识之中的认证数据和校验数据进行验算，以达到鉴别物品的真伪。下面，进一步说明物品防伪数据认证的工作过程。

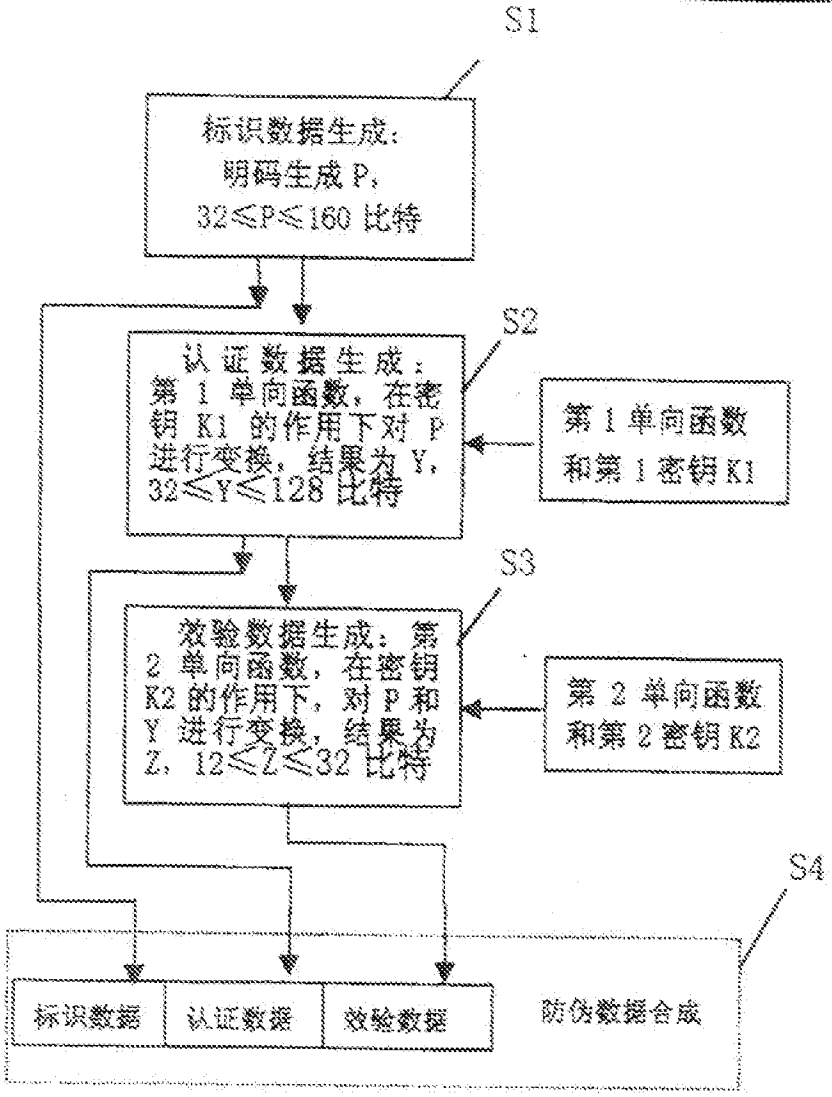
图 5 表示了应用本说明所述的物品防伪认证方法的一个可能的物品防伪网络的示意图。该网络是一个集中式认证网络。全国设置一个或多个认证中心，用于集中进行认证。将在本发明的认证装置中使用的第 1 单向函数，即对认证数据认证部分放置在认证中心。在各城市设置一个或多个城市分中心，用于将本城市通过电话或计算机或扫描设备录入的防伪数据集中传输至各认证分中心。同时，将本发明的认证装置中使用的第 2 单向函数，即对校验数据验证部分放置在城市分中心，对本城市分中心录入的防伪数据进行校验，并将校验通过的防伪数据集中传输至各认证分中心。

物品数据认证防伪的方法主要用于：产品防伪，将物品防伪数据结合于单个产品的标签、包装、容器，多件产品的大包装上，完成防伪认证；商品防伪，将物品防伪数据结合于单个商品的标签、包装、容器，多件商品的大包装上，完成防伪认证；证件防伪，将证件上的文字、图象用数据、字符、

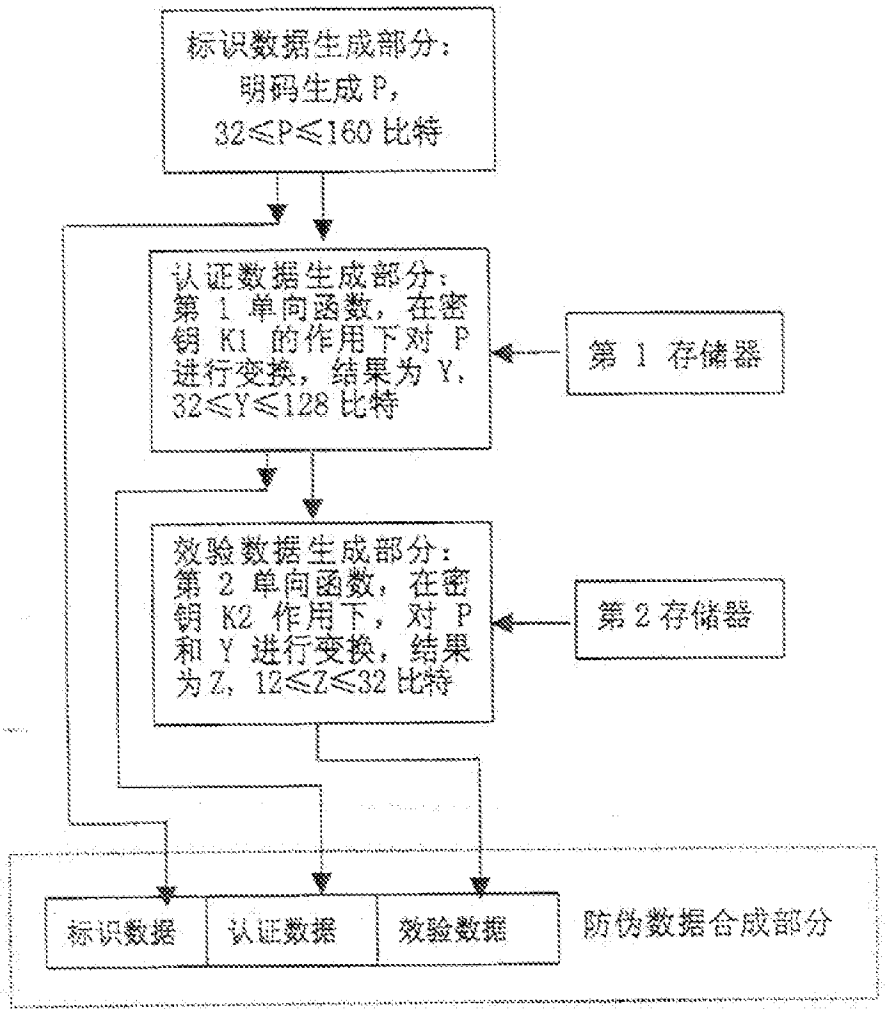
条码表示，利用物品数据认证防伪技术对这些数据、字符、条码进行全部或部分密码变换，获取认证数据、校验数据，将密码变换结果（也是数据）和获取的数据印制在证件上，或这些数据制作标签粘贴在证件上，利用本系统查询即可完成对证件的实时防伪认证；以及票据防伪，将票据上的文字、图象用数据、字符、条码表示，利用物品防伪数据技术对这些数据、字符、条码进行全部或部分密码变换，获取认证数据、校验数据，将密码变换结果（也是数据）和获取的数据印制在票据上，或这些数据制作标签粘贴在票据上，利用本系统查询即可完成对证件的实时防伪认证等等。

上面，已经参照各附图，对本发明的最佳实施例进行了详细描述，以便使本发明变得更清楚，而不应认为本发明仅仅限于上述的实施例。本领域的技术人员，通过上述各实施例的启迪，不难对本发明作出各种改进、改变或替换，因而这些改进、改变或替换，不应认为已脱离了本发明的构思，或附属权利要求书所限定的范围。

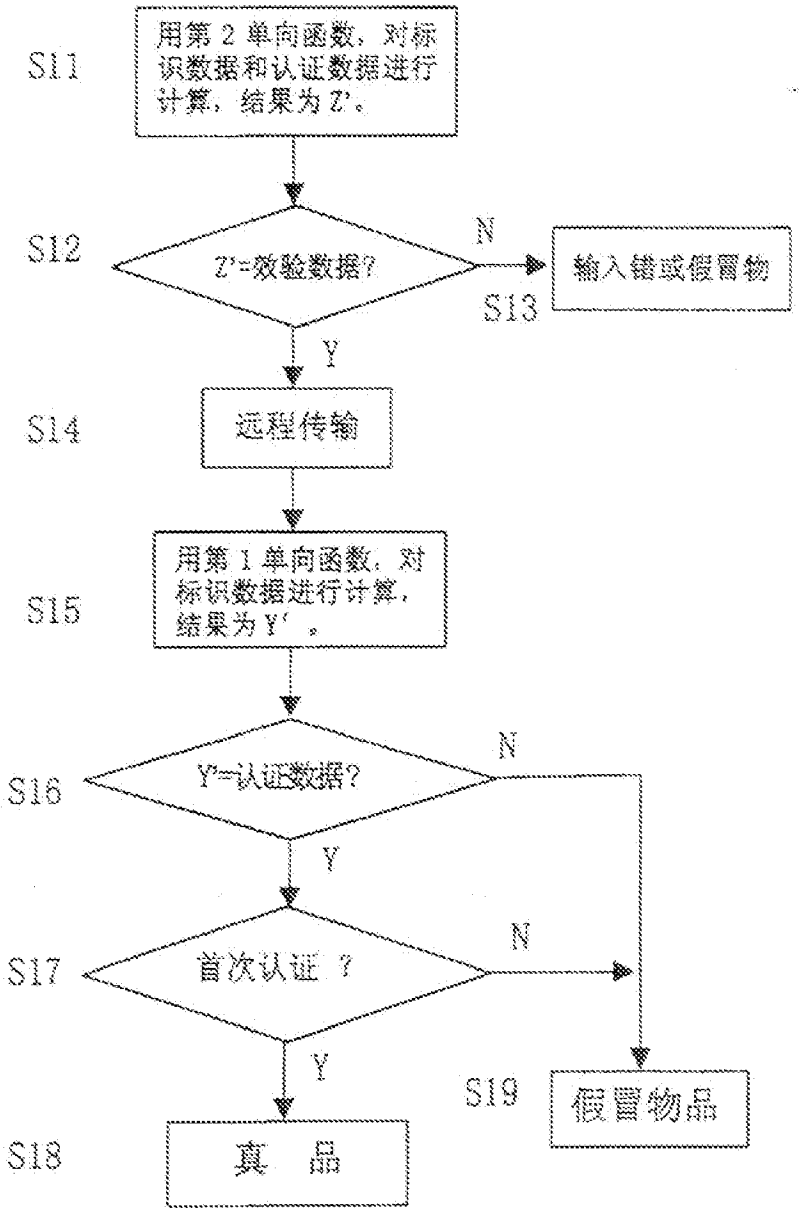
说 明 书 附 图


S1
标识数据生成：
明码生成 P，
32≤P≤160 比特
S2
认证数据生成：
第 1 单向函数，在密钥 K1 的作用下对 P 进行变换，结果为 Y，
32≤Y≤128 比特
第 1 单向函数
和第 1 密钥 K1
S3
效验数据生成：第 2 单向函数，在密钥 K2 的作用下，对 P 和 Y 进行变换，结果为 Z，12≤Z≤32 比特
第 2 单向函数
和第 2 密钥 K2
S4
标识数据
认证数据
效验数据
防伪数据合成

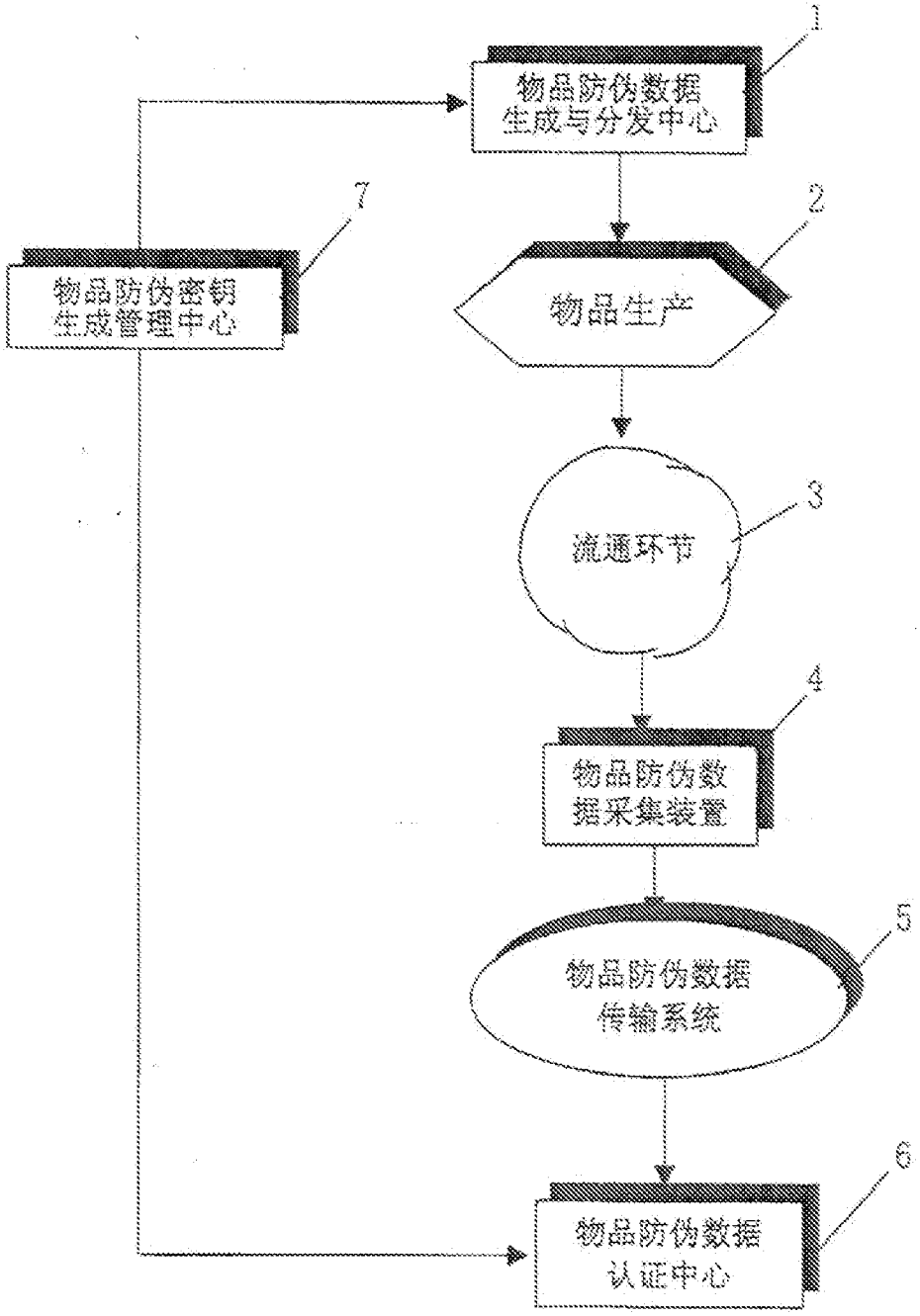
说明书图 1


标识数据生成部分：
明码生成 P，
32≤P≤160 比特
认证数据生成部分：第 1 单向函数，在密钥 K1 的作用下对 P 进行变换，结果为 Y，32≤Y≤128 比特
第 1 存储器
效验数据生成部分：第 2 单向函数，在密钥 K2 作用下，对 P 和 Y 进行变换，结果为 Z，12≤Z≤32 比特
第 2 存储器
标识数据
认证数据
效验数据
防伪数据合成部分

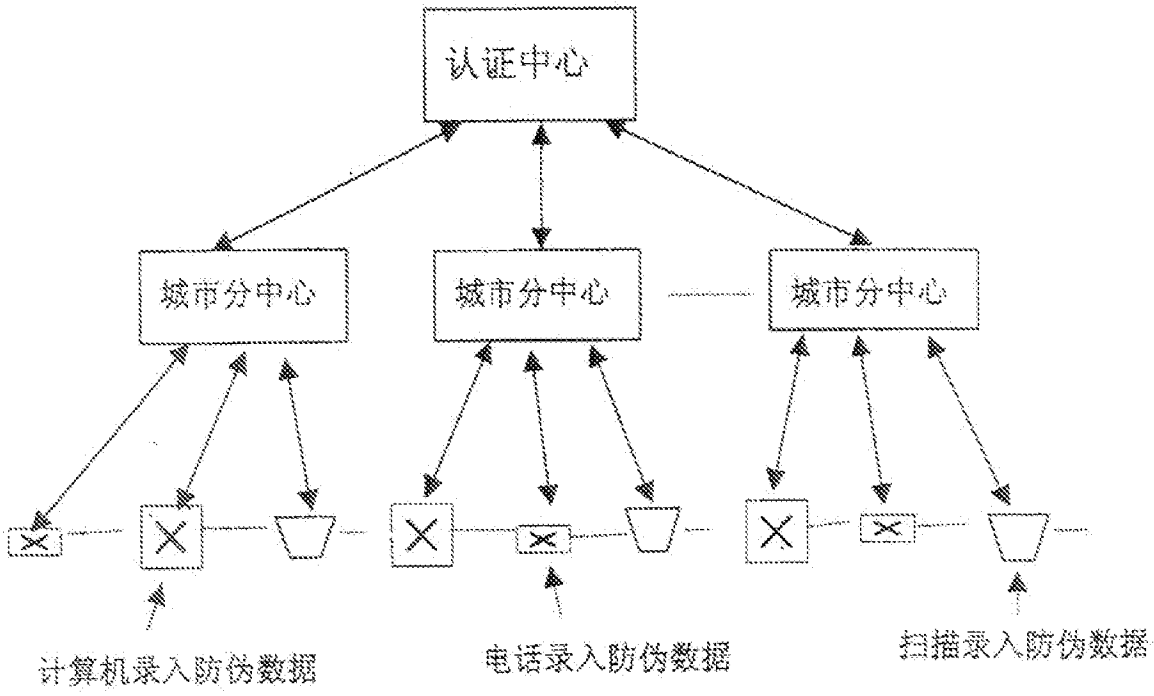
说明书图 2


S11
用第 2 单向函数，对标识数据和认证数据进行计算，结果为 Z'。
S12
Z'=效验数据?
N
S13
输入错或假冒物
Y
S14
远程传输
S15
用第 1 单向函数，对标识数据进行计算，结果为 Y'。
S16
Y'=认证数据?
N
Y
S17
首次认证 ?
N
Y
S18
真 品
S19
假冒物品

说明书图 3


1
物品防伪数据
生成与分发中心
2
物品生产
3
流通环节
4
物品防伪数
据采集装置
5
物品防伪数据
传输系统
6
物品防伪数据
认证中心
7
物品防伪密钥
生成管理中心

说明书图 4



说明书图 5